

Cyber-Physical Resilience Tool Step-by-step Training Guide

CPR Incident Reporting Module
ATOS/EVIDEN, Spain



Overview of the Cyber-Physical Resilience Tool

- + **CPR (Cyber-Physical Resilience) Tool** is developed under the SUNRISE project to enhance the cybersecurity posture of critical infrastructure (CI), particularly during complex events like pandemics. It aims to support security teams in managing digital threats that may arise alongside other challenges such as staff shortages or operational disruptions.
- + **CPR integrates multiple modules** to provide a holistic view of cyber threats. These include an anomaly detection system validated with real CI logs, a risk assessment module that incorporates temporary conditions and physical activity alarms, and a threat intelligence scoring component enhanced with source confidence evaluation.
- + **The tool aligns with known frameworks** such as MITRE ATT&CK for mapping Indicators of Compromise (IoCs), helping security analysts understand attack patterns more efficiently. It also includes features that support NIS 2 Directive compliance through its structured incident reporting module.
- + **The CPR dashboard** enables users to access risk reports, simulate mitigation strategies, and evaluate the effectiveness of cyber defense mechanisms in real-time. It is designed for ease of use, allowing operators to visualize and respond to threats across cyber and physical domains quickly and effectively.
- + **CPR is especially valuable for operators of essential services**, offering capabilities that strengthen incident awareness, improve response times, and support decision-making during both normal operations and crisis scenarios.

Content Overview



SUNRISE

This step-by-step training guide provides an overview of the **CPR Incident Reporting Module**, part of the SUNRISE Cyber-Physical Resilience Tool. It is designed to help users understand and navigate the key features. It forms part of the training materials provided for the solution, alongside the [training video](#).

01

TheHive
Task Management

04

Risk Re-Evaluation
Process

02

Early Warnings &
Countermeasures

05

Data Conversion &
Report Generation

03

Countermeasures
Evaluation &
Integration

06

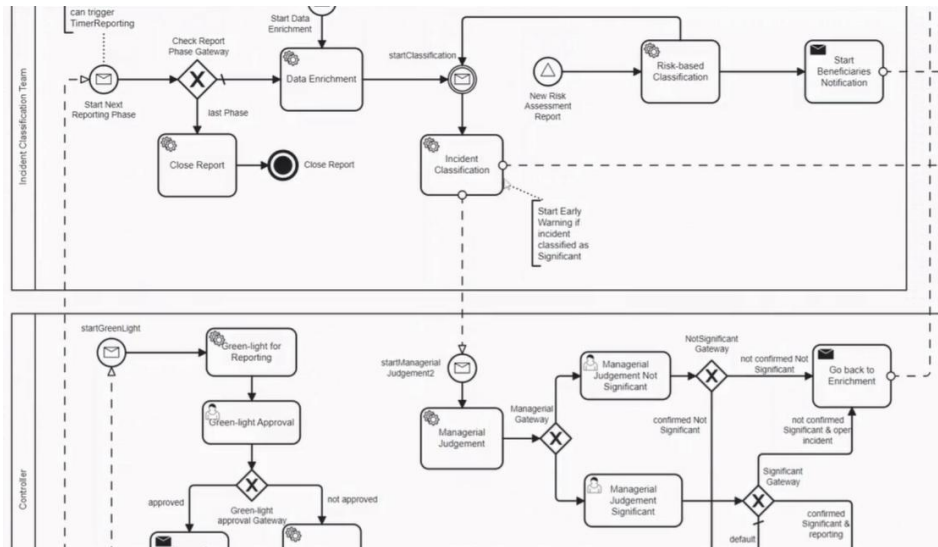
Review & Export
of Reports

TheHive Task Management

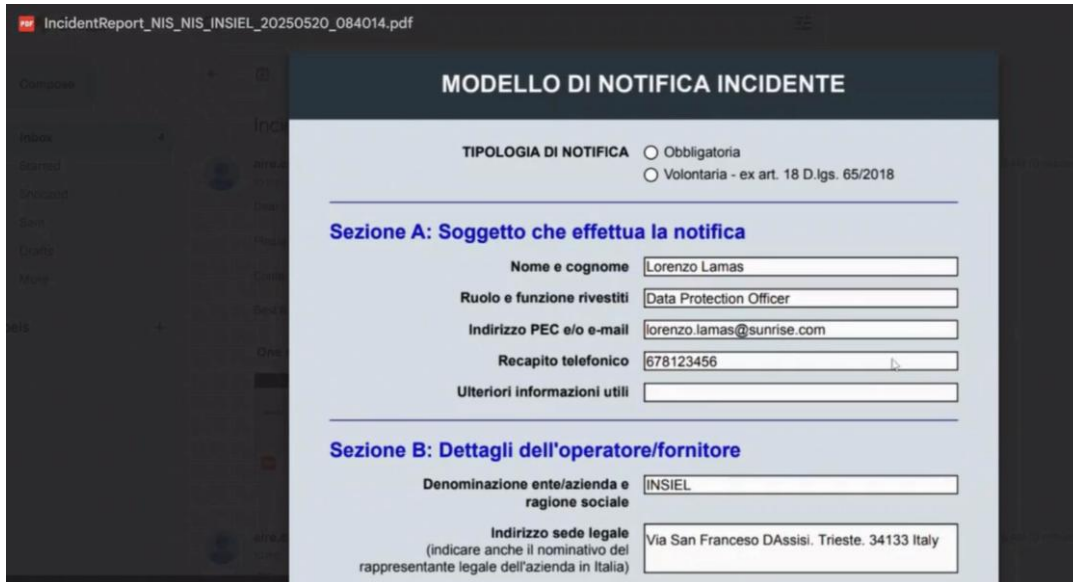
List of tasks (6 of 6)

Group	Task	Date	Assignee	Actions
IMT	Data Collection Closed after 2 minutes	05/20/25 10:26	Incident Management Team	
IMT	Notify Vulnerability Started 13 minutes ago	05/20/25 10:27	Incident Management Team	
IMT-ICLT	Data Enrichment Closed after 4 minutes	05/20/25 10:28	Incident Classification Team	
ICLT	Incident Classification Closed after 7 minutes	05/20/25 10:33	Incident Classification Team	
CONTROLLER	Managerial Judgement Started a few seconds ago	05/20/25 10:40	Controller	
IMT	Register countermeasures Started a few seconds ago	05/20/25 10:40	Incident Management Team	

- Upon registering an incident, tasks are **automatically created in TheHive** following the BPMN-defined workflow.
- Tasks include stages such as **incident classification**, **managerial judgement**, and **risk re-evaluation**.
- Once the classification is confirmed, a **managerial review task** is launched to validate or adjust the classification decision.



Early Warning & Countermeasures Trigger



IncidentReport_NIS_NIS_INSIEL_20250520_084014.pdf

MODELLO DI NOTIFICA INCIDENTE

TIPOLOGIA DI NOTIFICA ☐ Obbligatoria
☐ Volontaria - ex art. 18 D.lgs. 65/2018

Sezione A: Soggetto che effettua la notifica

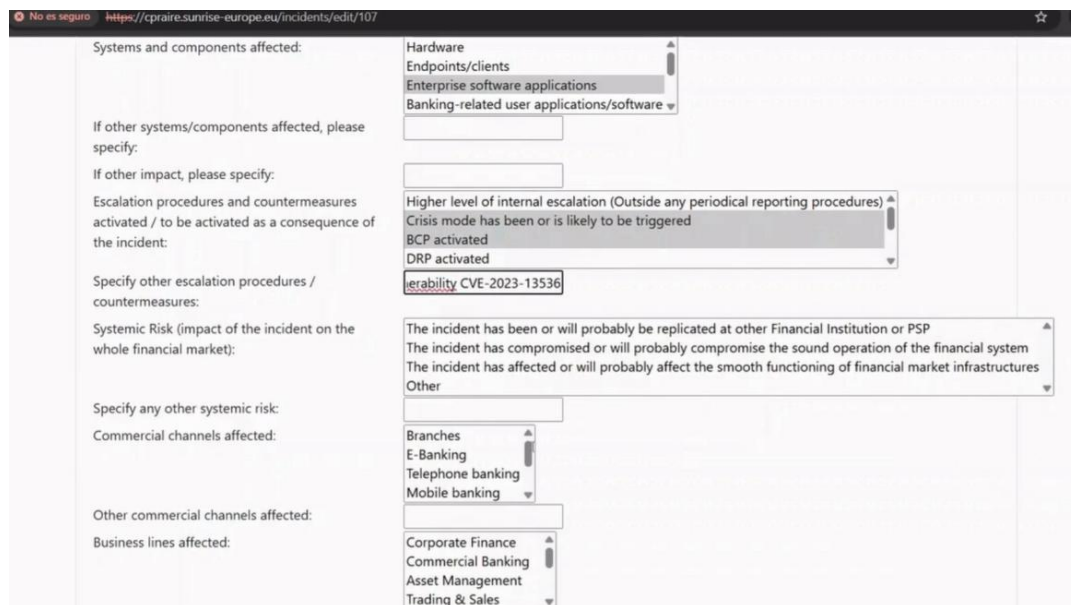
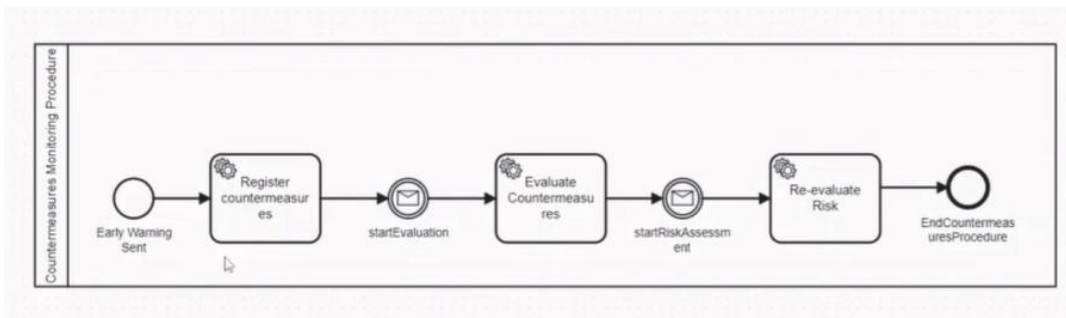
Nome e cognome
Ruolo e funzione rivestiti
Indirizzo PEC e/o e-mail
Recapito telefonico
Ulteriori informazioni utili

Sezione B: Dettagli dell'operatore/fornitore

Denominazione ente/azienda e ragione sociale
Indirizzo sede legale (indicare anche il nominativo del rappresentante legale dell'azienda in Italia)

- + If the incident is classified as **Significant**, an **Early Warning** is triggered according to the **NIS2 directive**.
- + An automatic **notification email** is sent to:
 - › **Service beneficiaries**
 - › **Supervisory Authorities**
- + Emails are configured through the CPR dashboard, with the **initial report PDF** automatically attached.

Countermeasures Evaluation & Integration



The screenshot shows the SUNRISE incident management interface. The URL bar indicates the page is for editing incident 107. The form includes sections for 'Systems and components affected', 'Escalation procedures and countermeasures activated / to be activated as a consequence of the incident', 'Specify other escalation procedures / countermeasures', 'Systemic Risk (impact of the incident on the whole financial market)', 'Specify any other systemic risk', 'Commercial channels affected', 'Other commercial channels affected', and 'Business lines affected'. The 'Systems and components affected' dropdown is open, showing options like 'Hardware', 'Endpoints/clients', 'Enterprise software applications', and 'Banking-related user applications/software'. The 'Escalation procedures' dropdown is also open, showing options like 'Higher level of internal escalation', 'Crisis mode has been or is likely to be triggered', 'BCP activated', 'DRP activated', and 'Incident severity CVE-2023-13536'.

- + **Countermeasures tasks** are generated after the Early Warning.
- + Countermeasures received from CSIRTs can be:
 - › Logged in **TheHive**
 - › Registered via the **AIRE dashboard**
- + Once evaluation is complete, tasks are closed, and a **new risk report is triggered**.
- + Risk re-evaluation is handled by the **CPR Risk Assessment module** and can be visualised in the dashboard.

Risk Re-Evaluation Process



```
[15cbe59bbdc:/opt/kafka/bin/.:/kafka-console-consumer.sh --bootstrap-server localhost:9092
--topic sunrise-alerts
{"alert": {"timestamp": "2025-05-20T10:24:26.372+0000", "rule": {"level": 6, "description":
"SQL injection attempt", "id": "31171", "firsttimes": 1, "last": false, "groups": ["web",
"accesslog", "attack", "sqlinjection"], "pcids": ["6.5", "11.4", "6.5.1"], "gdpr": ["1",
"V.35.7.d"]}, "agent": {"id": "002", "name": "sunrise-ci0-wza2", "ip": "10.44.19.151"}, "ma
nager": {"name": "webui.manager"}, "id": "174692696", "full_log": "www.example.com:80 1.1.1.1:
- [20/May/2025:10:24:12 +0000] \"GET /example/dirmas6orderMcd6Pr9f;select%20pg_sleep(9.703);%20
~%20example5101 HTTP/1.1\" 200 10345 \"https://www.example.com/\" \"Mozilla/5.0 (Windows NT 6.1; Win64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Sa
fari/537.21\" \"-\" \"Xief50n2nc7y0Kcrgp6d0wAAAMV\", \"decoder\": {\"parent\": \"web-accesslog\",
\"name\": \"web-accesslog\"}, \"data\": {\"protocol\": \"GET\", \"srcip\": \"1.1.1.1\", \"id\": \"200\",
\"url\": \"/example/dirmas6orderMcd6Pr9f;select%20pg_sleep(9.703);%20~%20example5101\",
\"location\": \"/var/log/nginx/access.log\"}}
DEBUG 2025-05-20 08:44:21.121 pika.heartbeats _send_heartbeat_frame
DEBUG 2025-05-20 08:44:21.122 pika.adapters.select_connection.call_later
201 : call_later: added timeout <pika.adapters.select_connection.Timeout
object at 0x7f24efb257b0> with deadline=1747730691.1213074 and callback=bound method He
artbeatChecker.send_heartbeat of <pika.heartbeats.HeartbeatChecker object at 0x7f24ef9dbb
0>; now=1747730661.1213074; delay=30.0
DEBUG 2025-05-20 08:44:21.153 pika.heartbeats _send_heartbeat
DEBUG 2025-05-20 08:44:21.153 pika.heartbeats _send_heartbeat_frame
DEBUG 2025-05-20 08:44:21.153 pika.adapters.select_connection.call_later
201 : call_later: added timeout <pika.adapters.select_connection.Timeout
object at 0x7f24efb242e0> with deadline=1747730691.1538122 and callback=bound method He
artbeatChecker.send_heartbeat of <pika.heartbeats.HeartbeatChecker object at 0x7f24efbab8
0>; now=1747730661.1538122; delay=30.0
INFO 2025-05-20 08:44:24.005 core.sing run
1309: Received message from Kafka: {"organization": "INSIEL", "source": "AI
E", "service": "health", "timestamp": "2025-05-20 08:44:24", "countermeasures": "Crisis mod
has been or is likely to be triggered;BCP activated;Applied patch to vulnerability CVE-
023-13530"}
DEBUG 2025-05-20 08:44:50.700 pika.heartbeats received
DEBUG 2025-05-20 08:44:50.700 pika.heartbeats received
DEBUG 2025-05-20 08:44:50.700 pika.heartbeats received
DEBUG 2025-05-20 08:44:50.700 pika.heartbeats received
DEBUG 2025-05-20 08:44:50.700 pika.heartbeats received
DEBUG 2025-05-20 08:44:50.700 pika.heartbeats received
DEBUG 2025-05-20 08:44:51.015 pika.heartbeats _send_heartbeat
DEBUG 2025-05-20 08:44:51.015 pika.heartbeats _send_heartbeat_frame
DEBUG 2025-05-20 08:44:51.016 pika.adapters.select_connection.call_later
201 : call_later: added timeout <pika.adapters.select_connection.Timeout
object at 0x7f24efb242e0> with deadline=1747730721.0159876 and callback=bound method He
artbeatChecker.send_heartbeat of <pika.heartbeats.HeartbeatChecker object at 0x7f24ef9dbb
0>; now=1747730691.0159876; delay=30.0
DEBUG 2025-05-20 08:44:51.076 pika.heartbeats _send_heartbeat
```

- + Risk updates are sent via **Kafka** messages to the CPR Risk Assessment module.
- + The system updates the **risk status** (e.g., from high to medium).
- + **CERCA dashboard** provides additional granularity on:
 - › Asset-level risks
 - › Impact of applied countermeasures

Risk assessment +			
Risk Model	Qualitative	Typical Loss	Worst Case
WRP6: Session Fixation	medium	555.0€	7200.0€
WRP8: SQL Injection	medium	45850.5€	664982.9€

Data Conversion & Report Generation



+ After closing the managerial judgement task, a **Data Conversion task** is launched in TheHive.

+ This triggers automatic generation of reports for:

› NIS2

› GDPR

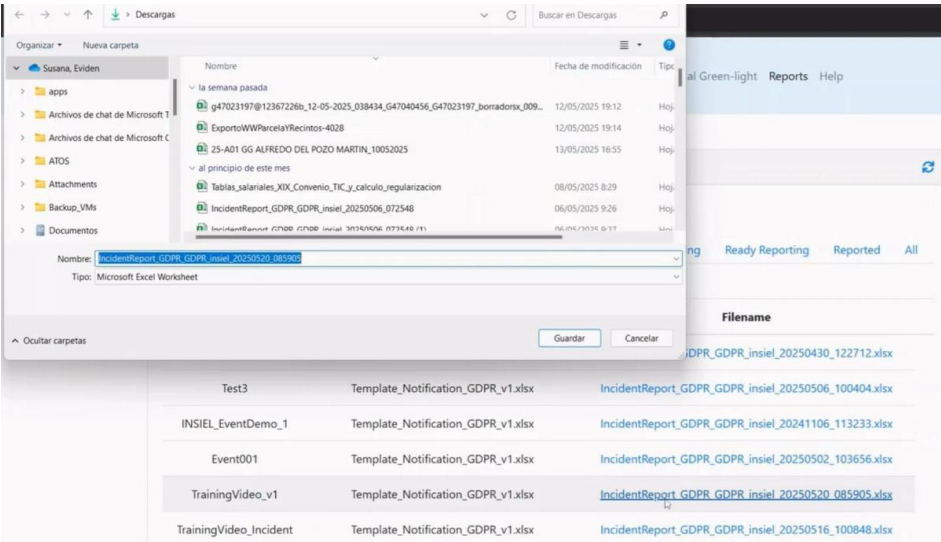
+ The **Incident Reporting Data Converter Responder** creates tailored reports with:

- › Incident details
- › Indicators of Compromise (IOCs)
- › Risk assessment summaries

List of tasks (8 of 8)

<input type="checkbox"/>	Group	Task	Date	Assignee	Actions
<input type="checkbox"/>	✔ IMT	▼ Data Collection Closed after 2 minutes	05/20/25 10:26	Incident Management Team	
<input type="checkbox"/>	🔔 IMT	▼ Notify Vulnerability Started 28 minutes ago	05/20/25 10:27	Incident Management Team	
<input type="checkbox"/>	✔ IMT-ICLT	▼ Data Enrichment Closed after 4 minutes	05/20/25 10:28	Incident Classification Team	
<input type="checkbox"/>	✔ ICLT	▼ Incident Classification Closed after 7 minutes	05/20/25 10:33	Incident Classification Team	
<input type="checkbox"/>	✔ IMT	▼ Register countermeasures Closed after 3 minutes	05/20/25 10:40	Incident Management Team	
<input type="checkbox"/>	✔ IMT	▼ Evaluate Countermeasures Closed after a few seconds	05/20/25 10:44	Incident Management Team	
<input type="checkbox"/>	✔ CONTROLLER	▼ Managerial Judgement Closed after a few seconds	05/20/25 10:55	Controller	
<input type="checkbox"/>	🔔 IRT	▼ Data Conversion Started a few seconds ago	05/20/25 10:55	Incident Reporting Team	

Review & Export of Reports



Cause of data breach	
System, software, service and IT infrastructure affected by the data breach	ImpactedComponents: Enterprise software applications; ;
Nature of the incident (device lost or stolen / paper lost or stolen or left in insecure location / mail lost or opened / hacking / malware / etc)	SQL injection
Circumstances in which the breach was discovered (Internal notification of the loss of hardware, internal incident management procedure, external notification, etc)	EventDetection: IT security ;
Type of breached data (Regular data; Special categories of data)	personaldata_category: Contact data; ;
How many data subjects are affected by the personal data breach, if applicable?	0
Categories of data subjects affected (customers, employees, patients, children, etc.)	datasubject_category: Employees; ;
What preventive measures have been specifically taken to protect the data disclosed?	Integrity breach
Action taken and active at the moment of the data breach, adopted to grant personal data security	
Actions planned and / or already taken to address the personal data breach / to address and mitigate the personal data security breach	
Actions planned and / or already taken to prevent similar	

- + Reports are accessible from the **AIRE dashboard** and include:
 - › **Excel (GDPR):** General info, breach specifics, IOCs, and risk analysis.
 - › **PDF (NIS2):** Summary report, with annexes listing IOCs and risk reports.
- + Reports are ready for submission to Supervisory Authorities.



SUNRISE

Thank you for following the training.

For more information:
<https://sunrise-europe.eu/>



This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101073821

The material presented and views expressed here are the responsibility of the author(s) only.
The EU Commission takes no responsibility for any use made of the information set out.